JC20 Rec'd PCT/PTO 26 JUL 2001

FORM PTO-1390 (REV. 11-2000) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY 'S DOCKET NUMBER	
018926-003800US	
U.S. APPLICATION NO. (If known, see 37 CFR 1 5)	
09/890179	

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US00/02101	January 28, 2000	January 29, 1999

TITLE OF INVENTION: AUTHENTICATION ENFORCEMENT USING DECRYPTION AND AUTHENTICATION IN A SINGLE TRANSACTION IN A SECURE MICROPROCESSOR

APPLICANT(S) FOR DO/EO/US
PAUL MORONEY

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST submission of items concerning a filing under 35 U.S.C. 371.**
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 36 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 37(c)(2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau
   c. ☒ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3)).
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.2 and 35 U.S.C. 1.821 – 1.825.
18. ☐ A second copy of the published international application under 36 U.S.C.
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information:

3 sheets formal drawings

I/S/ Application no. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/890179	PCT/US00/02101	018926-003800US

21. ☒ The following fees are submitted:

	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492(A) (1) – (5)):		
Neither international preliminary examination fee (37 CFR 1.492) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search report prepared by the EPO of JPO **$860.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)(4) **$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$690	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	2 - 20 =		x **$18.00**	$	
Independent claims	2 -3 =		x **$80.00**	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **270.00**	$	
TOTAL OF ABOVE CALCULATIONS =				$690	
☐ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. +				$	
SUBTOTAL =				$690	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFT 1.492(f).				$	
TOTAL NATIONAL FEE =					
Fee for recording the enclosed assignment (37 CFR 1.2(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$	
TOTAL FEES ENCLOSED =				$690	
				Amount to be refunded:	$
				charged:	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 20-1430 in the amount of $690 to cover the above fees.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 20-1430. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Charles J. Kulas
Townsend and Townsend and Crew LLP
Two Embarcadero Center, 8th fl.
San Francisco, CA 94111

SIGNATURE

Charles J. Kulas
NAME

35,809
REGISTRATION NUMBER

AUTHENTICATION ENFORCEMENT USING DECRYPTION AND AUTHENTICATION IN A SINGLE TRANSACTION IN A SECURE MICROPROCESSOR

CROSS-REFERENCES TO RELATED APPLICATIONS

This application claims priority from U.S. Provisional Patent Application Serial No. 60/117,788 filed on January 29, 1999 and from U.S. Provisional Patent Application Serial No. 60/128,772 filed on April 9, 1999, the disclosures of which are incorporated in their entirety herein by reference for all purposes.

BACKGROUND OF THE INVENTION

This invention relates in general to secure data processing in digital systems and more specifically to a device that performs decryption and authentication using a secure processor.

Public key systems have become a very popular means for providing security in digital systems. Public Key Systems (PKS) have two different keys, one for encryption, or signing, and one for decryption, or verifying. This separation of keys has great security value in that the sign/decrypt function can be securely isolated from verify/encrypt functions, as is appropriate for the typical use of these keys. Public key systems are also known as asymmetric systems, or cryptosystems, as opposed to non-public key systems that are known as symmetric, or secret key, systems.

To send a message in a public key system, a sender obtains the receiver's public key. The sender uses the public key to encrypt a message. The encrypted message is then sent to the receiver. Since only the receiver has the corresponding private key of the

public/private key pair, only the intended receiver can decrypt and view the encrypted message.

However, a problem arises in that the sender may not be sure that they have obtained the receiver's correct public key in the first place. For example, a fraudulent public key may have been provided under the guise of the receiver's public key. In order to prevent this, "certificates" are used to generate confidence in the legitimacy of a public key. A certificate is typically the information that is included along with a signed message, where the certificate includes the public key required to verify the signature on the message. The certificate is signed with the certifying authority's private key and can be verified by a recipient of the certificate by using the certifying authority's public key. Of course, the same problem of obtaining the known certifying authority's correct public key in the first place still exists. A sequence of certified public keys can be obtained from sources of progressively higher trust, where each preceding certificate's public key comes from a successively more trustworthy source. At some point, the user of a certificate's public key must be able to trust, or be assured that, the original public key for the chain of certificates does, indeed, come from the proper source and is valid.

The act of user authentication (verification of user identity) usually includes the verification of the user's certificate. Usually the certificate includes the identity of the sender, the identity of the certificate issuer, the sender's public key, the time period for which the certificate is valid, etc.

Sometimes it is necessary to update key pairs by sending new key pairs from one device to another. This procedure can benefit from being validated by certificates, but where the updating occurs frequently the inclusion of certificate processing can put a high processing burden on the participating systems. Also, certificates need to be generated, signed and transferred in order to minimize the effect that a "broken" or "stolen" private key could have on a system. The maintenance of security based on a public key scheme, certificates, authentication, etc., is referred to as a system's Public Key Infrastructure (PKI). An example of telecommunications systems where the implementation of a traditional PKI is problematic or prohibitive is in a large scale digital network, such as the Internet. Where the data being transferred is high bandwidth using many transactions of small size, the number of

discrete exchanges of data, along with their corresponding encryption, decryption, authentication, etc., is extremely large. However, the need for security such as is provided by a PKI is also great, especially in applications such as telephony, or other secure data transfers such as banking, etc.

Devices that process secure, or encrypted, information often use secure processors, or microprocessors, that are designed to prevent intrusion into, and unwanted tampering or misuse of, the processor. A problem with secure processors is that they must be tightly controlled by a manufacturer, or "owner," of the processor, or device within which the processor resides. Thus, it is difficult to provide an "open architecture" for third party developers, customers, etc., of the devices. One way to alleviate this problem is to include both a secure processor and an "unsecure processor" (or, simply, "processor"). The unsecure processor has lowered security that allows third party developers to have relatively free access to the processor and the processor's resources such as memory, support chips, etc., so that the third party can develop and install software to upgrade or change the device's functionality. Typically, the unsecure processor attends to systems and control functions and makes calls to, or requests of, the secure processor to decrypt messages, authenticate information and perform other security functions. In this role, the unsecure processor is also referred to as a "host" processor.

However, a problem with the host processor/secure processor approach is that it can reduce the overall security of the device. This is because the host processor has control over which messages, or other information, are submitted to the secure processor for decryption. Since the host processor can easily be reprogrammed, or otherwise controlled or "hacked" to perform security breaches, care must be taken that such breaches do not occur.

For example, in applications where a secure processor is called upon to perform authentication and decryption operations, the host processor is in a role of sending, or not sending, the information to the secure processor. Where the host processor makes requests of the secure processor for authentication, the host processor can be reprogrammed to "skip" the authentication operation, or to falsely state that the authentication operation was successful when, in fact, the authentication was not successful or never occurred.

Also, some systems use messages that are authenticated but not encrypted. This approach allows the host processor to have access to the contents of the unencrypted, "clear text," of the message whether or not the authentication is verified.

Thus, it is desirable to provide a device that overcomes one or more of the shortcomings of the prior art.

SUMMARY OF THE INVENTION

The present invention uses a secure processor operating with a host processor to perform a unitary decrypt/authenticate operation. The host processor receives encrypted messages that include authentication information. The host processor must submit each message to the secure processor. The secure processor then decrypts and authenticates the message. If authentication is not successful, the secure processor does not return the fully-decrypted message back to the host. In a preferred embodiment, the host will receive no part of the message upon failure.

In one embodiment the invention provides a method for performing authentication of messages in a device, wherein the device receives encrypted messages, wherein the device includes a host processor coupled to a secure processor. The method includes receiving an encrypted message; using the secure processor to decrypt the message; using the secure processor to authenticate the message; and subsequent to the steps of using the secure processor, performing the step of determining whether the message is authentic and, if the message is authentic, then transferring the decrypted message to the host processor.

In another embodiment the invention provides a method of providing secure processing in a telecommunications sytem that transfers messages to devices, wherein one or more of the devices include a host processor and a secure processor and wherein a message has an associated authentication. The method includes encrypting the message and associated authentication.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a flowchart showing basic steps of the present invention;

Fig. 2A shows a portion of a telephony network; and

Fig. 2B shows details of a cable telephony adapter.

DESCRIPTION OF THE SPECIFIC EMBODIMENTS

The present invention is preferably included in a device referred to as a Cable Telephone adapter (CTA). The CTA is used in a cable telephony system that is described in detail in the priority documents referenced at the beginning of this specification. Although specific reference is made to a cable telephony system, the invention is adaptable for use in virtually any telecommunications system that uses secured transactions.

Cable Telephony Adapter

FIG. 2A shows a portion of an IP telephony network 100 constructed in accordance with the present invention. The network 100 includes a first user 102 coupled to a source CTA 104. The source CTA 104 is further coupled to a source gateway controller 106 and an IP telephony network backbone 110.

The network 100 also includes a second user 112 coupled to a destination CTA 114. The destination CTA 114 is further coupled to a destination gateway controller 116 and the IP telephony network backbone 110. In addition, the network 100 also includes a customer service representative (CSR) center 120, a provisioning server 122 and a billing host 124.

Each user of the network 100 goes through an initialization process to activate network service. For example, when the user 102 and associated CTA 104 are coupled to the network, a series of messages are exchanged between the CTA 104, provisioning server 122, gateway controller 106 and the CSR 120. The messages provide for activation of telephony service for the user 102, establishment of account information and creation of encryption keys to be used by the CTA to encrypt and decrypt messages exchanged over the network. The billing host 124 is used to setup account information for each user and to bill for network

usage. The provisioning server 122 is used to initialize and register CTA devices within a specific IP telephony network.

Fig. 2B shows an exemplary embodiment of the CTA 104 constructed in accordance with the present invention. The CTA 104 includes a cable input interface (I/F) 202, a cable output I/F 204, a user output I/F 206, a user input I/F 208, a host processor 210, a memory 212 and an additional secure processor 220 along with secure memory 222, used to protect public/private key pairs 224. Certificates 214 are stored in regular memory because they are signed and don't require additional protection.

The cable input I/F 202 is coupled to a cable telephony input 216. The cable output I/F 204 is coupled to a cable telephony output 218. The cable telephony input and output I/F couple the CTA 200 to a cable telephony network, such as by connecting to a cable modem (not shown) that is coupled to the cable telephony network. In another embodiment, the cable modem is included in the CTA so that the cable telephony network may be connected directly to the CTA.

The processor 210 couples to the cable input I/F 202 and the cable output I/F 204 to provide processing of information received and transmitted, respectively, on the telephony network. The line 216 carries secure encrypted and/or signed information which cannot be processed directly by the host processor, since it does not have access to cryptographic keys. This includes provisioning information , call set-up and voice data. In cases where it is desired to perform secure authentication the host processor has to pass on this information to the secure processor, which has access to the necessary keys to perform cryptographic operations. The connections between the cable I/F modules and the user I/F modules carry unencrypted information. The unencrypted information is commonly referred to as clear text, which extends back to the user. Similarly, some clear text user input may need to be encrypted and/or signed securely. This cannot be done directly by the host processor. It passes on the information to the secure processor that performs the cryptographic operations. This way, encrypted and/or signed data appears on line 218.

The certificates in 214 cryptographically bind each public key to an identity. The short, self-signed public key may be bound to either the device or user identity, while the longer public keys installed at the time of manufacture must be bound to the identity of the

device (since the user identity is unknown at that time). The certificates are not protected in secure memory because they are already cryptographically protected with a digital signature.

Combined Decryption/Authentication

Fig. 1 is a flowchart that describes the basic steps of the present invention.

In Fig. 1, message 12 is received by a device such as the CTA of Figs. 2A and 2B. Message 12 includes message information 14 and signature 16.

Step 18 represents receipt of the message at the device. Transfer to, and receipt of, the message can be by any means. For example, the radio-frequency transmission, hardwire, fiber optic, acoustic, etc., channels can be used. Any suitable telecommunications network can be employed such as the Internet, cable television, satellite, telephone, etc. Any suitable protocols can be used. Receipt is performed by Cable Input Interface 202 of Fig. 2B. Upon receipt, the message is under the control of host processor 210. Other embodiments can use other means to receive the message. For example, the message can be provided directly to secure processor 220 without the need for host processor 210 to mediate.

Once received, step 20 is executed where the host processor transfers the message to the secure processor and requests decryption. Steps 24, 26 and 28 are performed by the secure processor and the secure processor's resources, as indicated by box 22.

At step 24, the secure processor performs authentication. In this case, signature 16 is verified by processing it with a public key. Other forms of authentication are possible. E.g, Symmetric key authentication, public key encryption, etc., are possible variations. At step 26 a check is made as to whether the authentication passed. If not, an error condition exists and the host processor will not receive the same information as when authentication passes. In the preferred embodiment, the host processor receives notification that the authentication failed. The host processor will receive no decrypted information in the message. Other embodiments may inform other devices in the system that an authentication has failed. Also, some of the encrypted information can still be decrypted and transferred to the host. This may be useful for service or troubleshooting as where a key has expired and the secure processor gives notice of the expiration date of a key, certificate, etc.

Assuming authentication passed, step 28 is executed by the secure processor to perform decryption on the message. Note that this embodiment uses an overall encryption on the message. Since decryption and verification keys are held only by the secure processor, and it supports only a single decryption and authentication operation, it is impossible to separate the two at the host processor level where the information is still encrypted. After decryption, the message information is sent to the host processor at step 30. Finally, the host processor can direct that some or all of the message information (or other information generated in response to the message information) be further processed.

Variations are possible from the arrangement shown in Fig. 1. For example, decryption can be performed before a check for authentication. In one form the signature could be encrypted and then must be decrypted before the authentication step can be performed. However, in another embodiment the message can be decrypted at the same time the signature is verified. If authentication then fails, the decrypted message can be discarded. This is not a security threat because the decrypted message is stored in secure memory 222. There may be speed advantages in such parallel processing.

Note that steps can be added to, or taken away from, the arrangement shown in Fig. 1. For example, step 20 of the host processor requesting the decryption can be omitted where the messages automatically are sent to the secure processor for decryption. Additional steps such as storing of the message, stripping of header information or data fields, etc., can be performed before, after, or during secure processing.

Thus, although the invention has been presented with respect to specific embodiments thereof, these embodiments are merely illustrative, and not restrictive, of the invention, the scope of which is to be determined solely by the appended claims.

WHAT IS CLAIMED IS:

1. A method for performing authentication of messages in a device, wherein the device receives encrypted messages, wherein the device includes a host processor coupled to a secure processor, the method comprising

receiving an encrypted message;

using the secure processor to decrypt the message;

using the secure processor to authenticate the message; and

subsequent to the steps of using the secure processor, performing the step of determining whether the message is authentic and, if the message is authentic, then transferring the decrypted message to the host processor.

2. A method of providing secure processing in a telecommunications sytem that transfers messages to devices, wherein one or more of the devices include a host processor and a secure processor, wherein a message has an associated authentication, the method comprising

encrypting the message and associated authentication.

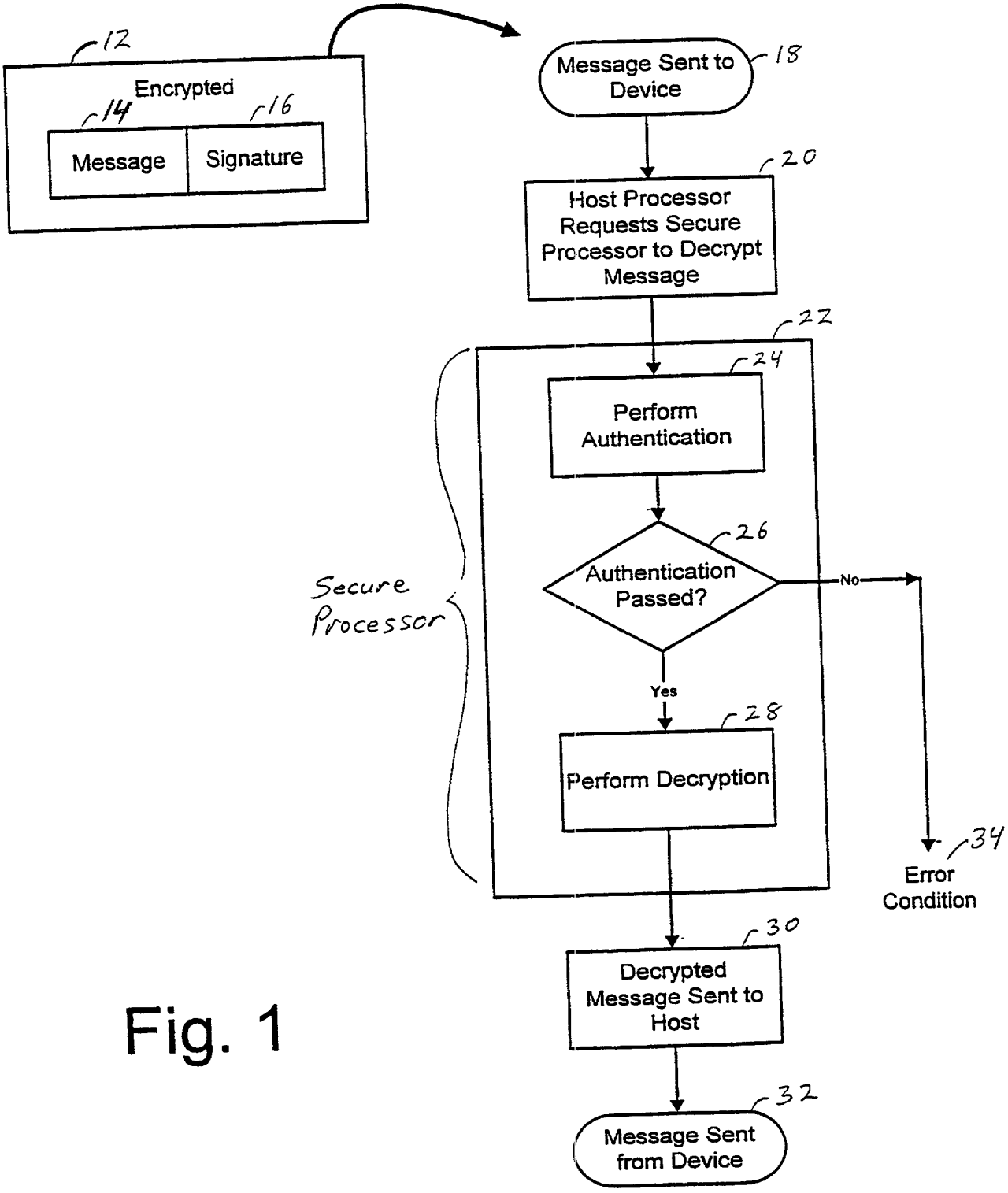
12
Encrypted
14
16
Message
Signature
Message Sent to Device
18
20
Host Processor Requests Secure Processor to Decrypt Message
22
24
Perform Authentication
26
Authentication Passed?
No
Yes
Secure Processor
28
Perform Decryption
34
Error Condition
30
Decrypted Message Sent to Host
32
Message Sent from Device

Fig. 1

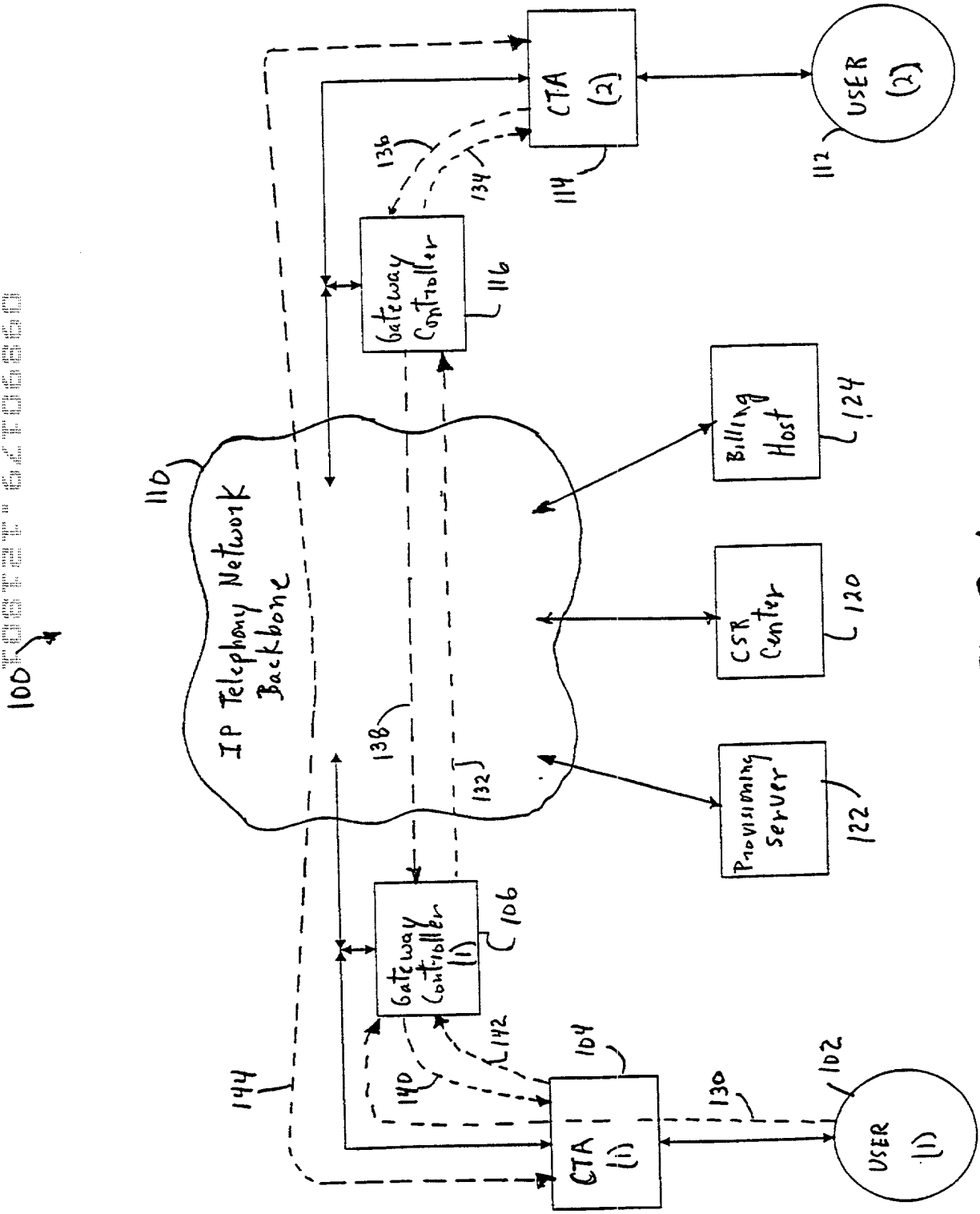
100
IP Telephony Network Backbone
110
Gateway Controller (2)
116
Gateway Controller (1)
106
CTA (2)
114
CTA (1)
104
USER (2)
112
USER (1)
102
Billing Host
124
CSR Center
120
Provisioning Server
122
130
132
134
136
138
140
142
144

FIG. 2A

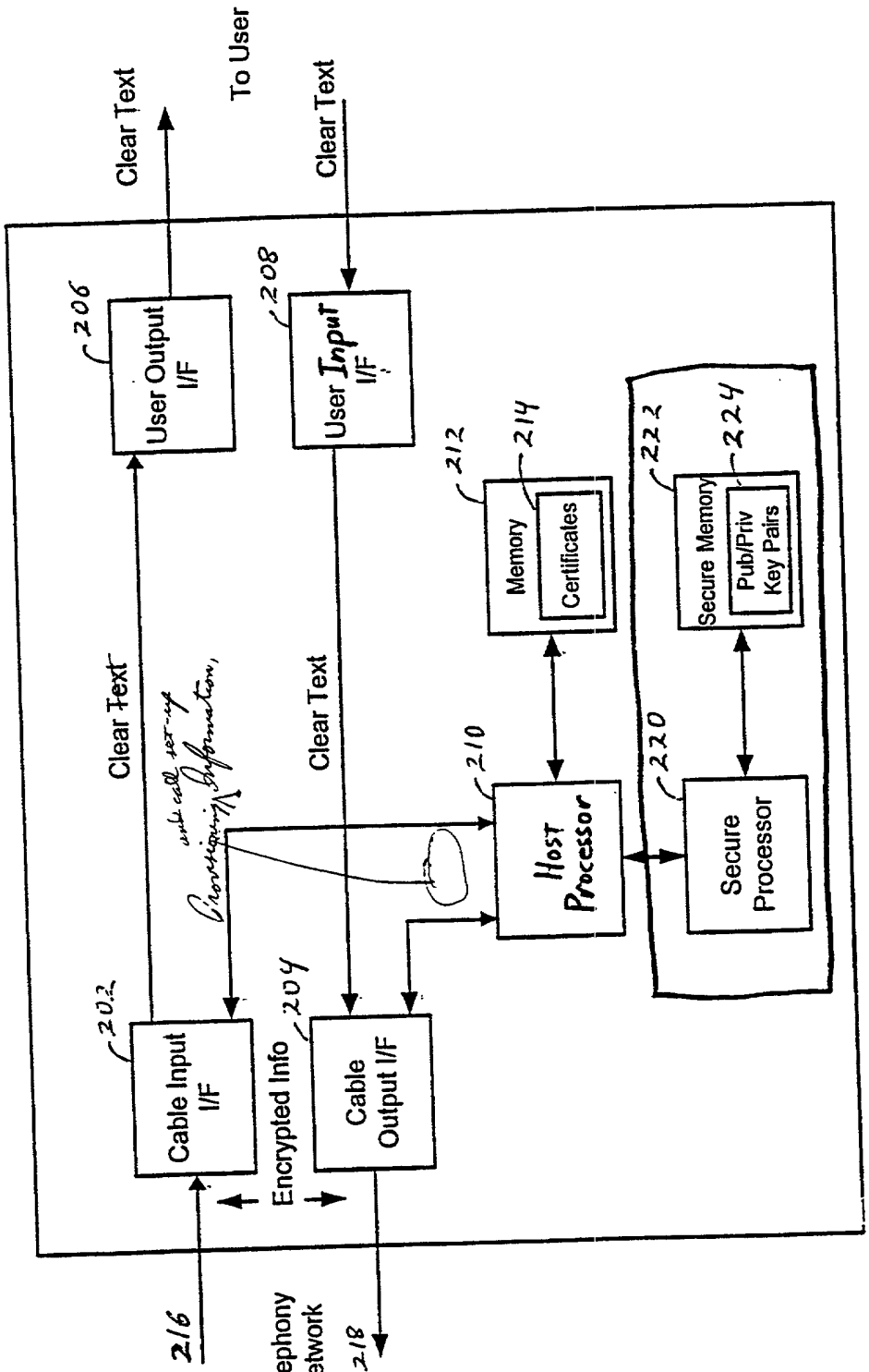
102
Clear Text
To User
Clear Text
206
User Output I/F
208
User Input I/F
212
214
Memory
Certificates
222
224
Secure Memory
Pub/Priv Key Pairs
Clear Text
Clear Text
Provisioning Information
210
Host Processor
220
Secure Processor
202
Cable Input I/F
204
Cable Output I/F
Encrypted Info
216
Telephony Network
218

Fig. 2B

Please type a plus sign (+) inside this box → [+]

PTO/SB/81 (02-01)
Approved for use through 10/31/2002. OMB 0651-0035
U.S. Patent and Trademark Office, U.S DEPARTMENT OF COMMERCE

Client Ref. D2433

POWER OF ATTORNEY OR AUTHORIZATION OF AGENT		
	Application Number	09/890,179, the National Phase of PCT/US00/02101, filed January 28, 2000
	Filing Date	
	First Named Inventor	Paul Moroney
	Title	AUTHENTICATION ENFORCEMENT USING DECRYPTION AND AUTHENTICATION IN A SINGLE TRANSACTION IN A SECURE MICROPROCESSOR
	Group Art Unit	
	Examiner Name	
	Attorney Docket Number	018926003800US

I hereby appoint:

☒ Practitioners at Customer Number 20350 → *Place Customer Number Bar Code Label here*

OR

☐ Practitioner(s) named below:

Name	Registration Number

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

☐ Practitioners at Customer Number →

☐ Firm *or* Individual Name					
Address					
Address					
City		State		ZIP	
Country					
Telephone		Fax			

I am the:

☐ Applicant/Inventor.

X Assignee of record of the entire interest. See 37 CFR 3.71.

Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

SIGNATURE of Applicant or Assignee of Record

Name	Charles M. Fish, Assistant Secretary
Signature	
Date	November 21, 2001

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of ____ forms are submitted.

SF 1292982 v1

DECLARATION

As a below named inventor, I declare that:

My residence, post office address and citizenship are as stated below next to my name; I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural inventors are named below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **AUTHENTICATION ENFORCEMENT USING DECRYPTION AND AUTHENTICATION IN A SINGLE TRANSACTION IN A SECURE MICROPROCESSOR** the specification of which ____ is attached hereto or _X_ was filed as **U.S. Application No. 09/890,179, the National Phase of PCT/US00/02101, filed January 28, 2000** and was amended on _____ (if applicable).

I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56. I claim foreign priority benefits under Title 35, United States Code, Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Country	Application No.	Date of Filing	Priority Claimed Under 35 USC 119

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below:

Application No.	Filing Date
60/117,788	January 29, 1999
60/128,772	April 9, 1999

I claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application No.	Date of Filing	Status

Full Name of Inventor 1.	Last Name: **MORONEY**	First Name: **PAUL**	Middle Name or Initial:	
Residence & Citizenship:	City: **Olivehain** CA	State/Foreign Country: **California**	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **3411 Western Springs Road**	City: **Olivehain**	State/Country: **California**	Postal Code: **92024**

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so

made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature of Inventor 1

Mr. Paul Moroney

Date 11-20-2006

SF 1292937 v1